RECEIVED
CENTRAL FAX CENTER
JUN 25 2004

Amendments to the Claims:

OFFICIAL

1. (Original) A database management apparatus, comprising:

an encryption key specification unit specifying whether a key for encryption of data of a column item of a database using a column key common among column items or a row key specific to each row;

an encryption unit encrypting each column item of the database using a key specified by said encryption key specification unit; and

a storage unit storing in memory the database encrypted by said encryption unit.

2. (Original) The apparatus according to claim 1, further comprising

a database search unit encrypting data input for retrieval using a row key common among predetermined column items when column items encrypted using the common row key is to be retrieved, comparing the encrypted retrieving data with each item data of the encrypted database stored in the memory, and performing retrieving process.

3. (Original) The apparatus according to claim 1, wherein said encryption unit encrypts data of a predetermined column item using a combination of a row key specific for each row and a column key common among corresponding column items.

4. (Original) The apparatus according to claim 1, wherein said encryption unit generates sequential vectors in a multidimensional space based on a predetermined function, and encrypting a database using the row key and the column key as a constant of the function in an encryption system using elements of the vectors as a key stream of encryption.

5. (Original) A database system which has a first information terminal containing a database, and a second information terminal requesting the first information terminal to search the database, and connects the first and second information terminals through a network, wherein:

on the first information terminal side, data of a first type of column item of the database is encrypted using a column key common among the column items, and data of a second type of column item is encrypted using a row key using a column key specific to each row;

when the second information terminal requests searching the database for the first type of column item, retrieving data input

is encrypted using a column key common among the column items, and the encrypted retrieving data is transmitted to the first information terminal through the network; and

on the first information terminal side, the encrypted database is searched using the retrieving data, and the encrypted data obtained as a search result is returned to the second information terminal through the network.

6. (Original) The database management apparatus which manages a database in which data is encrypted using a column key common among predetermined column items, comprising:

an encryption unit encrypting input retrieving data using the column key when data is retrieved from predetermined column items; and

a retrieval unit retrieving data by comparing the encrypted retrieving data with each item data of the encrypted database.

7. (Original) The apparatus according to claim 1, comprising:

a plaintext data obtaining unit obtaining plaintext data to be encrypted;

a vector generation unit sequentially generating vectors defined in a closed area of an n(n≥1)-dimensional space using a function determined using at least the column key or a row key;

and

a logical operation unit performing a logical operation in bits units using the plaintext data obtained by said plaintext data obtaining unit and elements of the vectors generated by said vector generation unit, and generating encrypted data.

8. (Original) A computer-readable storage medium storing a program used to direct a computer to perform the process, comprising:

encrypting data of a first type of column item of a database using a column key common among the column items, and encrypting data of a second type of column item using a row key specific for each row; and

searching encrypted database obtained as a result of the encrypting function.

9. (Original) A computer-readable storage medium storing a program used to direct a computer to perform the process, comprising:

encrypting input retrieving data using the column key when data is retrieved from predetermined column items; and

retrieving data by comparing the encrypted retrieving data with each item data of the encrypted database.

10. (Original) A database management apparatus, comprising:

a first encryption unit encrypting data of a first type of column item of a database using a column key common among the column items, and encrypting data of a second type of column item using a row key specific for each row;

a second encryption unit encrypting the row key used in encrypting the data of the second type of column item of the database by said first encryption unit using another key common among rows; and

a storage unit storing in memory the database encrypted by said first encryption unit with the row key encrypted by said second encryption unit.

11. (Original) The apparatus according to claim 10, wherein said row key is generated by a row number assigned to each row of said database and a random number.

12. (Original) An encryption apparatus according to claim 10, comprising:

a vector generation unit sequentially generating vectors defined in a closed area of an n(n≥1)-dimensional space using a function determined using each of the keys in the database management apparatus according to claim 10; and

a logical operation unit performing a logical operation in

bits units using the plaintext data obtained by said plaintext data obtaining unit and components of the vectors generated by said vector generation unit, and generating encrypted data.

13. (Original) A database system having a first terminal unit for managing a database, and a second terminal unit for searching the database independent of the first terminal unit, wherein:

on the first terminal unit side, the database is encrypted and the encrypted database is stored in a portable storage medium, and the storage medium is distributed; and

on the second terminal unit side, the encrypted database is searched using the distributed storage medium, and data obtained as a search result is decrypted and displayed.

14. (Original) The system according to claim 12, wherein:

said first terminal unit encrypts data of a first type of column item of the database using a column key common among the column items, encrypts data of a second type of column item using a row key using a column key specific to each row, and encrypts the row key using another key common among rows; and

said encrypted database is stored with the row key after the encryption in a storage medium.

15. (Original) The system according to claim 12, wherein said storage medium stores the encrypted database in said first terminal unit, and a predetermined program for searching encrypted database.

B1
A4

16. (Original) A computer-readable storage medium storing a program used to direct a computer to perform the process, comprising:

encrypting data of a first type of column item of a database using a column key common among the column items, and encrypting data of a second type of column item using a row key specific for each row; and

encrypting a row key used in encrypting data of a second type of column item of the database by said first encrypting function using another key common among rows.

Claims 17-29 (Canceled).